Department of Homeland Security Daily Open Source Infrastructure Report for 01 September 2006

Current Nationwide Threat Level is

ELEVATED
Significant Risk of Terrorist Attacks

For info click here
http://www.dhs.gov/

Daily Highlights

- The U.S. Food and Drug Administration is advising consumers not to purchase prescription drugs from Websites that sell counterfeit product filled by specific pharmacies in Manitoba, Canadia. (See item 20)
- The Department of Homeland Security announced Thursday, August 31, that more than 1,150 national, regional, state, and local organizations have joined the department to take part in National Preparedness Month in September. (See item 23)

Energy Sector

Current Electricity Sector Threat Alert Levels: Physical: ELEVATED, Cyber: ELEVATED
Scale: LOW, GUARDED, ELEVATED, HIGH, SEVERE [Source: ISAC for the Electricity Sector (ES−ISAC) − http://www.esisac.com]

1. *August 31, Associated Press* — **TXU to build nuclear plants.** Energy company TXU Corp. said Thursday, August 31, it plans to build nuclear power generators at one to three sites to help power Texas. The company said it expects to submit applications to the Nuclear Regulatory Commission in 2008 to build and operate the plants, which would likely begin operating between 2015 and 2020.
   Source: http://biz.yahoo.com/ap/060831/txu_nuclear.html?.v=1

2.

August 31, Platts Energy Bulletin — **NERC submits cybersecurity grid standards for FERC approval.** The North American Electric Reliability Council (NERC) submitted 16 new and 11 revised reliability standards to the Federal Energy Regulatory Commission (FERC) late Wednesday, August 30. "The largest number of them are what we refer to as the cybersecurity standards," said Stan Johnson, NERC's manager for situation awareness and infrastructure security. The commission approved NERC to be the electric reliability organization (ERO) in July after Congress in the Energy Policy Act of 2005 ordered the agency to supervise an electric reliability organization that develops standards and enforces the country's new mandatory reliability system. In its application to be the ERO, NERC in April submitted 102 existing voluntary reliability standards. FERC staff released a report in May citing deficiencies in those standards. "These are additional standards that had been in progress and have been working through the drafting teams and were not included in the 102," Johnson said. Cybersecurity standards relate to the control systems and "the possibility of hackers getting into the control systems" and compromising the reliability of the bulk power system," Johnson said. Source: http://www.platts.com/HOME/News/7683435.xml?sub=HOME&p=HOME/News&?undefined&undefined

[Return to top]

Chemical Industry and Hazardous Materials Sector

3. *August 31, Times−Picayune (LA)* — **Chemical fumes put five in Louisiana hospital.** Fumes from Express Container Services in St. Rose, LA, forced the evacuation of the nearby St. Rose Travel Center on Tuesday, August 29, when fumes from the chemical dichlorobutene entered the restaurant's ventilation system. Five people were sent to the hospital as a result. Source: http://www.nola.com/news/t−p/metro/index.ssf?/base/news−16/1157009182225860.xml&coll=1

4. *August 31, KNBC−TV (CA)* — **Chemical fire at California business spreads to power line.** A three−alarm fire at a metal plating business in Paramount, CA, had firefighters battling exploding vats of chemicals for about an hour Thursday morning, August 31. The fire at Anaplex Corp. started just before midnight and eventually engulfed the roughly 50,000−square−foot building. A nearby power−line pole caught fire, draping wires into the flames. A crew from Southern California Edison temporarily shut the power off to the area. Source: http://www.msnbc.msn.com/id/14600850/

[Return to top]

Defense Industrial Base Sector

5. *August 31, Washington Post* — **As U.S.−Indian alliance grows, defense firms seek to profit.** After decades on the sidelines, U.S. defense contractors are eyeing India's growing military budget and aging arsenal as a multibillion−dollar opportunity that could help offset a projected slowdown in Pentagon weapons spending and extend production lines for such items as the F−16 fighter. India has been effectively closed to U.S. defense firms since the 1960s, initially because of its ties with the Soviet Union, and later under formal sanctions imposed in response

to nuclear weapons tests in 1998. Those sanctions were lifted in 2001, a decision given impetus by the September 11 attacks and the growing strategic alliance between the two countries. Several of the Pentagon's largest contractors have either opened new offices or beefed up existing ones in India and are part of an industry−wide wooing of military officials and business leaders there. At stake are contracts worth billions from a country with expanding economic and strategic ties to the United States. While not the largest foreign defense market, industry officials and analysts consider it one of the fastest growing. India's defense budget is expected to reach more than $23 billion this year, compared with about $13 billion in 2000, according to Teal Group Corp., a Fairfax, VA, research firm.
Source: http://www.washingtonpost.com/wp−dyn/content/article/2006/08/30/AR2006083003091.html

6. *August 29, Defense Industry Daily* — **India's CVC issues procurement guidelines for defense.** India's Central Vigilance Commission (CVC) has issued new directives on defense purchases which may seem somewhat familiar to observers in other countries, but may end up having an impact on several high−profile defense contracts. The CVC has asked the Defense Ministry to avoid single−vendor situations unless very exceptional circumstances exist, include standard contract terms in Request for Proposals (RFPs), not deviate or dilute qualitative requirements after RFPs are issued, and require performance bonds and warranty bonds.
Source: http://www.defenseindustrydaily.com/2006/08/indias−cvc−issues−procurement−guidelines−for−defense/index.php

[Return to top]

Banking and Finance Sector

7. *August 30, Federal Computer Week* — **Education data at risk again.** The Department of Education is a victim of data exposure for the second time in less than a month. DTI Associates, a professional services contractor based in Arlington, VA, acknowledged that two laptop computers were stolen August 11 from its Washington, DC, office. The laptops contained information on 43 reviewers who were assessing grant applications for Education’s Teacher Incentive Fund, said Bruce Rankin, vice president of DTI. The only personal data that may have been in the laptops were the educators’ Social Security numbers, used for payroll identification purposes, he said.
Source: http://www.fcw.com/article95848−08−30−06−Web

8. *August 29, Department of the Treasury* — **Treasury designation targets elusive North Valle cartel leader.** The Department of the Treasury's Office of Foreign Assets Control (OFAC) on Tuesday, August 29, added to its list of Specially Designated Narcotics Traffickers four individuals and two companies tied to Juan Carlos Ramirez Abadia, a leader of Colombia's North Valle drug cartel. These four individuals operate a Colombian pharmaceutical distribution company, Disdrogas Ltda., on behalf of Juan Carlos Ramirez Abadia. Also designated was a Colombian holding company named Ramirez Abadia y Cia. S.C.S. "Juan Carlos Ramirez Abadia has been one of the most powerful and most elusive drug traffickers in Colombia," said Adam J. Szubin, Director of OFAC. "Today we are exposing and taking action against elements of his financial network for the first time, including seemingly legitimate companies built upon narcotics proceeds."

Source: http://www.treasury.gov/press/releases/hp74.htm

9. *August 29, Websense Security Labs* — **Multiple phishing alert: Veridian Credit Union, First National Bank of Burleston, HFS Federal Credit Union.** Websense Security Labs has received reports of new phishing attacks. One attack targets customers of Veridian Credit Union. Users receive a spoofed e−mail message claiming that account details need to be confirmed. The e−mail provides a link to a phishing site that attempts to collect the user's account information. In another attack targeting customers of First National Bank of Burleston, users receive a spoofed e−mail message claiming that unless the services listed on the e−mail are renewed immediately they will be deactivated and deleted. The e−mail provides a link to a phishing site that attempts to collect the user's account information. Another attack targets HFS Federal Credit Union. Users receive a spoofed e−mail message claiming that a new security system has been implemented, and in order to benefit from it, account details will need to be confirmed. The e−mail provides a link to a phishing site that attempts to collect the user's account information.
Screen shots:
http://www.websense.com/securitylabs/alerts/alert.php?AlertI D=593
http://www.websense.com/securitylabs/alerts/alert.php?AlertI D=594
http://www.websense.com/securitylabs/alerts/alert.php?AlertI D=595
Source: http://www.websense.com/securitylabs/alerts/

[Return to top]

Transportation and Border Security Sector

10. *August 31, Agence France−Presse* — **Thousands could be grounded by U.S.−European Union air security differences.** Over 100,000 people a week could be stopped from flying unless the United States and the European Union (EU) strike a deal over the provision of sensitive information on passengers, the top industry body said Thursday, August 31. The EU's top court in May overturned a decision forcing airlines to supply data on European passengers to U.S. authorities as part of a security crackdown, giving the two sides until September 30 to reach a new agreement. The European Commission, the EU's executive body, wants a new deal after the European Court of Justice quashed the previous agreement, ruling that it was "founded on an inappropriate legal basis." Under the old agreement, airlines were required to provide the U.S. authorities with more than 30 pieces of data on passengers and crew, including credit card information, addresses and telephone numbers, 15 minutes before departure. The EU−U.S. accord was reached in 2004 as a number of aircraft were being prevented from entering the United States over concerns that suspicious passengers were aboard.
Source: http://www.usatoday.com/travel/flights/2006−08−31−EU−US−secu rity−spat_x.htm

11. *August 31, Washington Times* — **Irish airline to allow cell phones on flights.** A European airline plans to let passengers use their cell phones during flights starting next year, but it could be awhile before U.S. carriers get the green light from federal officials. Ryanair, the Irish budget airline and Europe's biggest low−cost carrier, intends to outfit 50 aircraft, or about a quarter of its fleet, with OnAir mobile technology by the end of next year, allowing passengers to call, text message and e−mail during flight. Ryanair's remaining fleet will be equipped starting in 2008. This would make Ryanair the first European airline to let passengers use their

cell phones in flight. In the United States, cell phone service on airborne aircraft is not specifically barred by the Federal Aviation Administration (FAA), but −− as with all portable electronic devices −− airlines would need to demonstrate that it does not interfere with a plane's communication and navigation systems, FAA spokesperson Les Dorr said. The FAA allows portable devices without radio transmitters, such as laptops or mp3 players, to be used at altitudes above 10,000 feet. In the meantime, the issue of cell phones onboard is moot since a Federal Communications Commission ban prevents it for fear that air−to−ground calls would overload the ground−based cell phone system.
Source: http://www.washtimes.com/business/20060830−115925−7545r.htm

12. *August 31, Associated Press* — **Jet's landing gear catches fire in Miami.** A jetliner's landing gear caught fire when two of its tires blew out on the runway at Miami International Airport, officials said. No one was injured, and the fire was quickly extinguished. The US Airways Boeing 737 had 94 passengers and six crewmembers, airport spokesperson Marc Henderson said. The escape slides were deployed from the plane's exits, and the passengers and crew were evacuated, officials said.
Source: http://www.chron.com/disp/story.mpl/ap/nation/4154809.html

13. *August 30, Government Accountability Office* — **GAO−06−819: Public Transportation: New Starts Program Is in a Period of Transition (Report).** The Safe, Accountable, Flexible, Efficient Transportation Equity Act: A Legacy for Users (SAFETEA−LU) authorized about $7.9 billion in commitment authority, through fiscal year 2009, for the Federal Transit Administration's (FTA) New Starts program, which is used to select fixed guideway transit projects, such as rail and trolley projects, and to award full funding grant agreements (FFGAs). The New Starts program serves as an important source of federal funding for the design and construction of transit projects throughout the country. SAFETEA−LU requires the Government Accountability Office (GAO) to report each year on FTA's New Starts process. As such, GAO examined (1) the number of projects that were evaluated, rated, and proposed for FFGAs for the fiscal year 2007 evaluation cycle and the proposed funding commitments for the fiscal year 2007 budget; (2) procedural changes that FTA proposed for the New Starts program beginning with the fiscal year 2008 evaluation cycle; and (3) changes SAFETEA−LU made to the New Starts program and FTA's implementation of these changes. GAO reviewed New Starts documents and interviewed FTA officials and project sponsors, among other things, as part of its review. GAO is not making recommendations in this report.
Highlights: http://www.gao.gov/highlights/d06819high.pdf
Source: http://www.gao.gov/cgi−bin/getrpt?GAO−06−819

14. *August 30, Reuters* — **Jetliner pilot locked out of cockpit.** The pilot of a Canadian airliner who went to the washroom during a flight found himself locked out of the cockpit, forcing the crew to remove the door from its hinges to let him back in, the airline said on Wednesday, August 30. The incident occurred aboard a flight from Ottawa to Winnipeg on Saturday, August 26. The regional jet, capable of carrying 50 people, was operated by Air Canada's Jazz subsidiary. Jazz spokesperson Manon Stewart said that with 30 minutes of the flight to go, the pilot went to the washroom, leaving the first officer in charge. But when he tried to get back into the cockpit, the door would not open. "The door malfunctioned ... this is a very rare occurrence," Stewart said, adding that the crew's decision to remove the door had been in line with company policy.

Source: http://www.cnn.com/2006/WORLD/americas/08/30/pilot.lockout.r eut/index.html

[Return to top]

Postal and Shipping Sector

15. *August 31, Associated Press* — **UPS pilots ratify higher paying contract.** Atlanta−based UPS pilots have approved a new contract with the world's largest shipping carrier that includes hefty pay raises, large signing bonuses, and higher health care premiums. The deal ends a lengthy battle that was mired by threats of a walkout. The Independent Pilots Association (IPA) said Thursday, August 31, that 56.5 percent of UPS pilots who voted approved of the deal, which runs through 2011. The deal, reached after more than three years of talks, together with a tentative agreement between FedEx Corp. and its pilots, furthers a trend in recent years that has seen pay for cargo airline pilots shoot up while the pay of many commercial airline pilots has declined. "The profit is so much greater in moving packages, freight, and cargo than in moving human beings," IPA spokesperson Brian Gaudet said. UPS pilots had been making on average more than $175,000 a year, according to the company. The new contract will boost average pilot pay to about $206,000 a year, UPS spokesperson Mark Giuffre said.
Source: http://biz.yahoo.com/ap/060831/ups_pilots.html?.v=5

[Return to top]

Agriculture Sector

16. *August 31, Agence France−Presse* — **Bluetongue virus spreads to France.** France has become the latest European country to report a case of bluetongue virus, in a dairy cow in the northern Ardennes region. The insect−borne disease was identified in a herd of 31 dairy cows in the town of Brognon, the agriculture ministry said in a statement. France has alerted the European Commission and the World Organization for Animal Health placed the herd under observation, the ministry said. Although bluetongue is frequently reported in southern Europe, the current outbreak −− first detected on August 17 in the southern Netherlands, later in Belgium and Germany −− is the first in northern Europe.
Bluetongue information: http://www.fao.org/AG/AGAINFO/subjects/en/health/diseases−cards/bluetongue.html
Source: http://news.yahoo.com/s/afp/20060831/hl_afp/francehealthfarm sheep_060831102800

17. *August 30, U.S. Department of Agriculture* — **Biotechnology report issued.** Deputy U.S. Department of Agriculture (USDA) Secretary Chuck Conner announced Wednesday, August 30, that a report about the future of biotechnology is available to the public. Prepared by USDA's Advisory Committee on Biotechnology and 21st Century Agriculture (AC21), the report describes the advances in agricultural biotechnology's first decade and discusses a range of topics related to agricultural biotechnology that may be addressed by the secretary over the next decade. The AC21 was established in 2003 to examine how biotechnology is likely to change agriculture and USDA's work over the long term. The 20−member committee represents a wide spectrum of views and interests and is composed of farmers, technology providers, academics, representatives from the food manufacturing and shipping industries, and

representatives from consumer and environmental organizations.
USDA's biotechnology portal:
http://www.usda.gov/wps/portal/!ut/p/_s.7_0_A/7_0_1OB?contentidonly=true&contentid=AC21Reports.xml
Source: http://www.usda.gov/wps/portal/!ut/p/_s.7_0_A/7_0_1OB?contentidonly=true&contentid=2006/08/0328.xml

[Return to top]

Food Sector

18. *August 30, Bay City News (CA)* — **Lettuce linked to E. coli outbreak.** Lettuce grown in Monterey, CA, has been linked to five cases of E. coli bacteria poisoning in the Ogden, UT−area in June, according to a Utah health official. The lettuce was served at a Wendy's restaurant in Ogden during a three−day period in late June and officials from the Health Department believe it is connected to the E. coli outbreak. "The only food item that was shared by all of these cases was iceberg lettuce from this Wendy's store," Health Officer Gary House said. Because Wendy's regularly disposes of its unused lettuce, health officials could not test samples of the lettuce from the three−day period to positively confirm the origin of the E. coli, according to House. E. coli is a bacterium that can cause a variety of illnesses, most commonly fever, abdominal cramps, nausea, vomiting, and watery or bloody diarrhea.
Source: http://cbs5.com/localwire/localfsnews/bcn/2006/08/30/n/HeadlineNews/LETTUCE−OUTBREAK/resources_bcn_html

[Return to top]

Water Sector

Nothing to report.
[Return to top]

Public Health Sector

19. *August 31, Voice of America* — **Indonesia struggles to contain bird flu.** Indonesia is struggling to contain the spread of the H5N1 bird flu virus in people and poultry. The country now has the world's largest number of human bird flu deaths, and critics say it needs to do more to eradicate the disease. But the government's efforts are hampered by limited resources and resistance from local communities. Indonesia faces unique challenges. Its population is spread over 17,000 islands, domestic fowl roam everywhere, and there is widespread resistance to the central government among many of its diverse cultures. John Weaver is an advisor on avian flu with the Food and Agriculture Organization, which is helping Indonesia fight the disease. He says Jakarta's culling program is not rigorous enough. In some cases only 30 or 40 percent of the birds in an area are killed because villagers do not cooperate. Weaver says getting the virus under control in Indonesia will require sustained support from donors. "It's not going to be a quick fix," he said. "It's not a one or two year program, it's a five to ten year program. And it's very resource dependent."

Source: http://www.voanews.com/english/2006−08−31−voa9.cfm

20. *August 30, U.S. Food and Drug Administration* — **Consumers warned not to buy or use prescription drugs from various Websites that sell counterfeit product.** The U.S. Food and Drug Administration (FDA) is advising consumers not to purchase prescription drugs from Websites that have orders filled by Mediplan Prescription Plus Pharmacy or Mediplan Global Health in Manitoba, Canada, following reports of counterfeit versions of prescription drug products being sold by these companies to U.S. consumers. FDA is investigating these reports and is coordinating with international law enforcement authorities on this matter. Laboratory analyses are underway for intercepted product that was destined for the U.S. market. Preliminary laboratory results to date have found counterfeits of the following drug products from these Websites: Lipitor, Diovan, Actonel, Nexium, Hyzaar, Ezetrol (known as Zetia in the U.S.), Crestor, Celebrex, Arimidex, and Propecia.
Source: http://www.fda.gov/bbs/topics/NEWS/2006/NEW01441.html

[Return to top]

Government Sector

Nothing to report.
[Return to top]

Emergency Services Sector

21. *August 31, Federal Emergency Management Agency* — **Federal Emergency Management Agency National Situation Update.** Tropical Activity: Atlantic/Gulf of Mexico/Caribbean Sea: At 5:00 a.m. EDT Thursday, August 31, the broad center of Tropical Storm Ernesto was located about 90 miles east−southeast of Jacksonville, FL and about 195 miles south of Charleston, SC. Ernesto was upgraded to a Tropical Storm at 11:25 p.m. Wednesday, August 30. Ernesto is moving toward the north near 15 mph. A gradual turn toward the north−northeast and a faster forward speed is expected during the next 24 hours. This motion will bring the center of Ernesto away from the coast of Florida and could bring the center near the South Carolina coast late Thursday night. Maximum sustained winds are estimated near 50 mph, with higher gusts. Strengthening is forecast during the next 24 hours. Central and Eastern Pacific: The National Hurricane Center is issuing advisories on dangerous category four Hurricane John, centered about 450 miles southeast of Cabo San Lucas, Baja California, and on Tropical Storm Kristy, centered about 790 miles southwest of the southern tip of Baja California. Neither of these systems will affect U.S. Territories or interests.
To view other Situation Updates: http://www.fema.gov/emergency/reports/index.shtm
Source: http://www.fema.gov/emergency/reports/2006/nat083106.shtm

22. *August 31, Providence Journal (RI)* — **Emergency notification system up and running for Rhode Island school district.** On Wednesday, August 30, parents of more than 11,000 Warwick, RI, students got a phone call and received a message from Superintendent Robert J. Shapiro. The phone call was a test of the district's new mass−messaging system with a welcome−back message before the first day of school. The system, to be used in case of

emergencies and when the district needs to get out other important information, allows Shapiro and other administrators to prerecord a voice message, and then set a time for it to be "delivered." At that time, the system will simultaneously call the homes or listed contact numbers for all of Warwick's students. The system would be ideal for times when the district needs to call off classes in the middle of the day, during a storm, for example, Shapiro said. But it would not be used in the early morning to warn of cancellations: the district will continue to rely on television and radio for that.
Source: http://www.projo.com/education/content/projo_20060831_w31apb .31f06eb.html

23. *August 31, Department of Homeland Security* — **DHS and coalition of more than 1,150 launch National Preparedness Month 2006.** The Department of Homeland Security (DHS) announced Thursday, August 31 that more than 1,150 national, regional, state and local organizations have joined the department to take part in National Preparedness Month. This nationwide effort encourages Americans to prepare for emergencies of all kinds in their homes, businesses, schools and communities. This year, the department is putting a particular focus on family emergency preparedness, reminding individuals to make themselves and their loved ones better prepared. Throughout September, DHS and coalition members are highlighting the importance of individual emergency preparedness and encouraging Americans to get an emergency supply kit, make a family emergency plan and be informed about the different types of emergencies that may affect them. The goal of National Preparedness Month is to educate Americans about the importance of emergency preparedness and encourage individuals to take action. Throughout the year, DHS promotes individual emergency preparedness through the Ready Campaign and Citizen Corps as part of a broader national effort conducted by the department's Directorate for Preparedness.
National Preparedness Fact Sheet: http://www.dhs.gov/dhspublic/display?content=5814
Source: http://www.dhs.gov/dhspublic/display?content=5815

24. *August 29, Fort Leavenworth Lamp (KS)* — **Exercise hones military response to nightmare scenarios.** At Fort Monroe, VA, Joint Task Force Civil Support (JTF−CS) is writing the way the U.S. military responds to dire circumstances, such as the scenario in Sudden Response 2006: a domestic terror attack involving an aerosol form of the plague bacteria. In the Joint Planning Group (JPG), procedures and lines of communication are plotted and established that will save lives if the scenarios ever become reality. Exercises such as Sudden Response 2006 allow the Department of Defense (DoD) to determine how military elements function in civil emergencies, what resources can be used, what are distractions and what must be avoided. Realistically refining the playbooks is the goal of exercises such as Sudden Response 2006, explained Paul Marcinko, deputy surgeon for JTF−CS. The JPG representatives must update the playbook with all of the scenario's potential issues and how each one would affect their counterparts in the field. The playbook explains how each issue was explored and becomes a resource for DoD civil disaster relief assistance efforts.
Source: http://www.ftleavenworthlamp.com/articles/2006/08/30/dod_new s/dod5.txt

[Return to top]

Information Technology and Telecommunications Sector

25.

August 31, Security Focus — **Mozilla Firefox FTP denial−of−service vulnerability.** Mozilla Firefox is prone to a denial−of−service vulnerability when making FTP connections. An attacker may exploit this vulnerability to cause Mozilla Firefox to crash, resulting in denial−of−service conditions.
For a complete list of vulnerable products: http://www.securityfocus.com/bid/19678/info
Solution: Currently, Security Focus is not aware of any vendor−supplied patches for this issue.
Source: http://www.securityfocus.com/bid/19678/references

26. *August 30, Security Focus* — **Microsoft Windows 2000 multiple COM object instantiation code execution vulnerabilities.** Microsoft Windows 2000 is prone to multiple memory corruption vulnerabilities that are related to the instantiation of COM objects. These issues may be remotely triggered through Internet Explorer. The vulnerabilities arise because of the way Internet Explorer tries to instantiate certain COM objects as ActiveX controls. This may result in arbitrary code execution, but this has not been confirmed. The affected objects are not likely intended to be instantiated through Internet Explorer.
For a complete list of vulnerable products: http://www.securityfocus.com/bid/19636/info
Solution: Currently, Security Focus is not aware of any vendor−supplied patches for this issue.
Source: http://www.securityfocus.com/bid/19636/references

27. *August 30, Security Focus* — **Latest polymorphism hides viruses better.** A virus that infects AMD64−based Windows systems uses some tricky techniques to make defensive reverse engineering more difficult, security firm Symantec said this week. The virus, dubbed W64.Bounds, is not spreading in the wild, but was submitted as a proof of concept to antivirus researchers. The program is not easy to detect because it encrypts itself using a new algorithm and exploits a Windows feature available only on AMD64 systems to control execution, Peter Ferrie, senior antivirus researcher for Symantec, said in a post on the company's research blog. "The AMD64 virus is both polymorphic and entrypoint obscuring," Ferrie stated in a second blog post. "The result is that it is not a simple matter to find the true start of the decryptor and to emulate from the wrong place can result in incorrect decryption."
Ferrie's blog postings: http://www.symantec.com/enterprise/security_response/weblog/2006/08/virus_qa_w3264bounds.html
http://www.symantec.com/enterprise/security_response/weblog/2006/08/polymorphism_comes_to_the_amd6.html
Source: http://www.securityfocus.com/brief/292

28. *August 30, VNUNet* — **Scientists claim first quantum cryptographic network.** U.S. scientists on Wednesday, August 30, claimed to have developed the world's first truly quantum cryptographic data network. By integrating quantum noise−protected data encryption (QDE) with quantum key distribution (QKD), researchers from the Northwestern University and BBN Technologies of Cambridge, MA, have developed a complete data communication system which boasts "extraordinary resilience to eavesdropping." The QDE method, called AlphaEta, makes use of the inherent and irreducible quantum noise in laser light to enhance the security of the system and make eavesdropping much more difficult. QKD exploits the unique properties of quantum mechanics to securely distribute electronic keys between two parties.
Source: http://www.vnunet.com/vnunet/news/2163177/boffins−plug−first −truly

Internet Alert Dashboard

Current Port Attacks

Top 10 Target Ports	1026 (win−rpc), 445 (microsoft−ds), 25 (smtp), 139 (netbios−ssn), 54856 (−−−), 113 (auth), 38809 (−−−), 32794 (−−−), 47290 (−−−), 6881 (bittorrent) Source: http://isc.incidents.org/top10.html; Internet Storm Center

To report cyber infrastructure incidents or to request information, please contact US−CERT at soc@us−cert.gov or visit their Website: www.us−cert.gov.

Information on IT information sharing and analysis can be found at the IT ISAC (Information Sharing and Analysis Center) Website: https://www.it−isac.org/.

[Return to top]

Commercial Facilities/Real Estate, Monument &Icons Sector

Nothing to report.
[Return to top]

General Sector

Nothing to report.
[Return to top]

DHS Daily Open Source Infrastructure Report Contact Information

DHS Daily Open Source Infrastructure Reports − The DHS Daily Open Source Infrastructure Report is a daily [Monday through Friday] summary of open−source published information concerning significant critical infrastructure issues. The DHS Daily Open Source Infrastructure Report is archived for ten days on the Department of Homeland Security Website: http://www.dhs.gov/iaipdailyreport

DHS Daily Open Source Infrastructure Report Contact Information

Content and Suggestions:	Send mail to dhsdailyadmin@mail.dhs.osis.gov or contact the DHS Daily Report Team at (703) 983−3644.
Subscription and Distribution Information:	Send mail to dhsdailyadmin@mail.dhs.osis.gov or contact the DHS Daily Report Team at (703) 983−3644 for more information.

Contact DHS

To report physical infrastructure incidents or to request information, please contact the National Infrastructure Coordinating Center at nicc@dhs.gov or (202) 282−9201.

To report cyber infrastructure incidents or to request information, please contact US−CERT at soc@us−cert.gov or visit their Web page at www.us−cert.gov.

Department of Homeland Security Disclaimer

The DHS Daily Open Source Infrastructure Report is a non−commercial publication intended to educate and inform